IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

ERIC O'BRIEN, individually and on behalf of all others similarly situated, Plaintiff, v. GEISINGER HEALTH and NUANCE COMMUNICATIONS, INC., Defendants.	Case No. _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Eric O'Brien ("Plaintiff"), individually and on behalf of all others similarly situated, by and through his undersigned counsel, brings this Class Action Complaint against Defendants Geisinger Health ("GH") and Nuance Communications, Inc. ("Nuance") (and collectively with GH, "Defendants"). Plaintiff alleges the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

INTRODUCTION

1. Healthcare providers and their business associates that handle sensitive, personally identifying information ("PII") or protected health information ("PHI") owe a duty to the individuals to whom that data relates. This duty arises because it

is foreseeable that the exposure of PII or PHI to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

2. The harm resulting from a data and privacy breach manifests in a number of ways, including identity theft and financial fraud, and the exposure of a person's PII or PHI through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

3. As a healthcare provider, GH knowingly obtains patient PII and PHI and has a resulting duty to securely maintain such information in confidence.

4. GH expressly recognizes its duty to safeguard patient PII and PHI, stating: "Geisinger is committed to protecting the privacy and confidentiality of its patients' and members' medical information."[1]

[1] *For Patients and Members HIPAA Notice of Privacy Practices*, GEISINGER, https://www.geisinger.org/about-geisinger/corporate/corporate-policies/hipaa (last visited August 19, 2024).

5. In the course of providing healthcare services to its patients, GH contracts with an outside vendor, Nuance, to provide certain information technology services to GH. Upon information and belief, in order to facilitate Nuance's provision of certain information technology services, GH transmits patient PII and PHI to Nuance.

6. Nuance provides artificial intelligence ("AI") software to healthcare providers across the United States and around the world. Nuance technology is used by 90% of hospitals and 10,000 healthcare organizations worldwide, and four out of five healthcare organizations within the United States.[2] The AI technology sold by Nuance includes transcription services, diagnostic analytics, document capture, speech recognition, and more.

7. Across these organizations, Nuance claims to transmit over 300 million "patient stories" (*e.g.*, radiology reports, clinician documentation of appointments) each year.[3] These "patient stories" inherently involve personal information gathered from those millions of patients.

8. Like GH, Nuance recognizes its duty to safeguard the PII and PHI it is entrusted. Nuance's HIPAA Privacy Policy states that "Nuance embraces a holistic

---

[2] *Healthcare AI Solutions & Services*, NUANCE, https://perma.cc/6PX5-P77E (captured June 5, 2024).

[3] *Fact Sheet: Nuance Healthcare by the Numbers*, NUANCE (2022), https://perma.cc/RTL2-9LCQ (captured June 5, 2024).

approach to securing patient data within our custody."[4] The Business Associate Agreement posted on Nuance's website also promises its customers that Nuance will "use appropriate safeguards . . . with respect to electronic protected health information, to prevent use or disclosure of PHI other than as provided for by this BA Agreement."[5]

9. Despite Defendants' commitments to safeguarding patient PII and PHI, their commitments nevertheless fell flat when a former Nuance employee was able to access and take patient records relating to over one million GH patients (the "Data Breach").[6]

10. Despite Defendants becoming aware of the Data Breach on November 29, 2023, they failed to notify Plaintiff and Class Members for approximately seven (7) months from their discovery of the Data Breach.

11. Plaintiff, on behalf of himself and the Class as defined herein, brings claims for negligence, negligence *per se*, breach of fiduciary duty, breach of confidences, unjust enrichment and declaratory judgment, seeking actual and

---

[4] *Global Privacy - HIPAA Requirements*, NUANCE, https://www.nuance.com/about-us/trust-center/privacy/hipaa.html (last visited August 19, 2024).
[5] *Business Associate Agreement*, NUANCE, https://www.nuance.com/about-us/terms-and-conditions/previous-versions/business-associate-agreement-20200624.html (last visited August 19, 2024).
[6] *Geisinger Provides Notice of Nuance's Data Security Incident* ("Notice"), GEISINGER (June 24, 2024), https://www.geisinger.org/about-geisinger/news-and-media/news-releases/2024/06/24/18/17/geisinger-provides-notice-of-nuances-data-security-incident.

putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

12. Based on the information provided by Defendants to date, a wide variety of PII and PHI was implicated in the Data Breach, including but not limited to, patient names in combination with one or more of the following: dates of birth, address, patient admission and discharge or transfer codes, medical record numbers, race, gender, phone numbers, and treatment facility name abbreviations.[7]

13. As a direct and proximate result of Defendants' inadequate data security, and their breach of their duty to handle PII and PHI with reasonable care, Plaintiff's and Class Members' PII and PHI has been accessed by an unauthorized third party and exposed to an untold number of unauthorized individuals.

14. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, intrusion of their health privacy, medical insurance fraud, and similar forms of criminal mischief—risk which may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

15. To recover from Defendants for these harms, Plaintiff and the Class seek damages in an amount to be determined at trial, declaratory judgment, and

[7] *Id*.

injunctive relief requiring Defendants to: (1) disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; (2) implement improved data security practices to reasonably guard against future breaches of PII and PHI possessed by Defendants; and (3) provide, at their own expense, all impacted victims with lifetime identity theft protection services.

PARTIES

16. Plaintiff Eric O'Brien is an adult, who at all relevant times, is and was a citizen of the Commonwealth of Pennsylvania.

17. Defendant Geisinger Health d/b/a Geisinger Health Foundation is a Pennsylvania corporation with a principal place of business located in Danville, Pennsylvania.

18. Defendant Nuance Communications, Inc. is a Delaware corporation with its principal place of business located in Burlington, Massachusetts.

JURISDICTION AND VENUE

19. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. At least one member of the Class defined below is a citizen of a different state than one of the Defendants, and there are more than 100 putative Class Members.

20. This Court has general personal jurisdiction over GH because GH is registered to do business, and maintains its principal place of business in Danville, Pennsylvania.

21. This Court has general personal jurisdiction over Nuance because Nuance is an out-of-state corporation registered to do business under the laws of the Commonwealth of Pennsylvania since March 2, 1998. As part of registering to do business in the Commonwealth of Pennsylvania, Nuance "shall enjoy the same rights and privileges as a domestic entity and shall be subject to the same liabilities, restrictions, duties and penalties . . . imposed on domestic entities." 15 Pa. C.S.A. § 402(d). Among other things, Pennsylvania law is explicit that "qualification as a foreign corporation under the laws of [the] Commonwealth" shall permit courts within Pennsylvania to "exercise general personal jurisdiction" over a registered foreign corporation just as they can over a domestic corporation. 53 Pa. C.S.A. § 5301(a)(2). Thus, by registering to do business in the Commonwealth of Pennsylvania and benefiting from the opportunity to do business in the Commonwealth of Pennsylvania, Nuance has consented to being subject to general jurisdiction in the Commonwealth of Pennsylvania.

22. In the alternative, this Court has specific personal jurisdiction over Nuance because Nuance purposely availed themselves of Pennsylvania by serving as a vendor that provides information technology services to GH.

23. Venue is proper in these District under 28 U.S.C. § 1391(b)(2) because GH is headquartered in this District, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. Defendants Collect and Store Patient PII and PHI.

24. GH is a healthcare provider that operates ten hospital campuses and 133 primary and specialty care clinics across Pennsylvania.[8]

25. Annually, GH serves the healthcare needs of over 600,000 patients.[9]

26. While administering healthcare services, GH receives, creates, and handles PII and PHI, which includes, *inter alia*, patients' names dates of birth, address, admit and discharge or transfer codes, medical record numbers, race, gender, phone numbers, and treatment facility name abbreviations.

27. Patients must entrust their PII and PHI to GH to receive healthcare services, and in return, they reasonably expect that GH will safeguard their highly sensitive information and keep their PHI confidential.

---

[8] *About Geisinger* (Statistics), GEISINGER https://www.geisinger.org/-/media/OneGeisinger/pdfs/GH/about-geisinger/pdfs/Geisinger-About-us-numbers_01.pdf?sc_lang=en&hash=D531FB9C831353305024148882FE0B47 (last visited Augusts 19, 2024); *see also*, Emily Olsen, *Data Breach at Geisinger May Have Exposed Data from 1.2M Patients*, INDUSTRY DIVE (July 2, 2024), https://www.healthcaredive.com/news/geisinger-nuance-communications-data-breach/720382/.

[9] *About Geisinger* (Statistics), *supra* note 8.

28. Upon information and belief, the PII and PHI GH receives, creates, and handles while administering healthcare services is entrusted to Nuance, one of GH's information technology providers.

29. Nuance provides AI software to healthcare providers across the United States and around the world. The AI technology sold by Nuance includes transcription services, diagnostic analytics, document capture, speech recognition, and more.[10]

30. Nuance's services are used widely within the healthcare industry; Nuance claims that its products are used by 77% of hospitals and 10,000 healthcare organizations worldwide.[11]

31. While providing its services to its contracting healthcare partners, including GH, Nuance receives, creates, and handles PII and PHI, which includes, *inter alia*, patients' names dates of birth, address, patient admit and discharge or transfer codes, medical record numbers, race, gender, phone numbers, and treatment facility name abbreviations.

32. By collecting and storing valuable PII and PHI that is routinely targeted by cybercriminals, Defendants have a resulting duty to implement adequate data

[10] *Healthcare AI Solutions & Services*, *supra* note 2.
[11] *Fact Sheet: Nuance Healthcare by the Numbers*, *supra* note 3.

security measures to safeguard Plaintiff's and Class Members' PII and PHI from unauthorized access.

33. Although Defendants have a duty to safeguard Plaintiff's and Class Members' PII and PHI, Defendants nevertheless employed inadequate data security measures to protect and secure the PII and PHI with which they were entrusted, resulting in the Data Breach and compromise of Plaintiff's and Class Members' PII and PHI.

B. Defendants are Subject to HIPAA.

34. As a health care provider, GH falls within the definition of a covered entity subject to the Health Insurance Portability and Accountability Act ("HIPAA").[12]

35. Additionally, because Nuance is contracted by covered entities, including GH, to provide services involving the transmission of PHI, Nuance qualifies as a business associate subject to HIPAA.[13]

36. Under HIPAA, Defendants are required to implement adequate safeguards to prevent unauthorized use or disclosure of PHI, including by implementing requirements of the HIPAA Security Rule.[14] Defendants are further

[12] *See* 45 CFR § 160.103.
[13] *Id.*
[14] The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained

required to report any unauthorized use or disclosure of PHI, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.[15]

37. Due to the nature of Defendants' businesses, they would be unable to engage in regular business activities without collecting and aggregating patient information that they know and understand to be sensitive and confidential.

38. Indeed, both Defendants explicitly claim to be compliant with HIPAA.

39. In GH's Notice of Privacy Practices, it explains to patients: "Under HIPAA, the information Geisinger collects about you as a patient is generally considered protected health information (PHI). Geisinger may only use and disclose your PHI pursuant to an authorization, or as otherwise permitted or required by law."[16]

40. GH further informs patients: "We are required by law to maintain the privacy and security of your PHI. We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information."[17]

---

by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. *See* 45 C.F.R. Part 160 and Part 164, Subparts A and C.

[15] *See* Breach Notification Rule, 45 CFR §§ 164.400–414.

[16] *Geisinger Notice of Privacy Practices*, GEISINGER (Dec. 1, 2021), https://www.geisinger.org/about-geisinger/corporate/corporate-policies/hipaa/notice-of-privacy-practices-ghs (last visited August 19, 2024).

[17] *Id.*

41. Nuance also claims to follow a stringent data security approach and states that it remains "firmly committed" to HIPAA compliance.[18]

42. Despite Defendants' assurances and duty to safeguard Plaintiff's and Class Members' PHI, Defendants employed inadequate data security measures to protect and secure the information with which they were entrusted, resulting in the Data Breach and subsequent compromise of Plaintiff's and Class Members' PHI.

43. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' sensitive information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' PHI from unauthorized access.

44. Further, given the application of HIPAA, and that Plaintiff and Class Members directly or indirectly entrusted their PHI to Defendants in order to receive healthcare services, Plaintiff and Class Members reasonably expected that Defendants would safeguard their highly sensitive information and keep their PHI confidential.

[18] *Global Privacy—HIPAA Requirements*, NUANCE, https://www.nuance.com/about-us/trust-center/privacy/hipaa.html (last visited August 19, 2024).

C. Defendants Knew of the Risks of Storing Valuable PII and PHI, and of the Foreseeable Harm to Their Patients if Their PII and PHI Were Exposed.

45. At all relevant times, Defendants knew they were storing sensitive PII and PHI and that, as a result, its systems would be attractive for cybercriminals.

46. Defendants also knew that a breach of their systems and exposure of the information stored therein would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

47. These risks are not theoretical; in the last year alone, numerous high-profile PII and PHI breaches have been reported to the Department of Health and Human Services at business such as Cencora (formerly AmerisourceBergen), Sav-Rx, Aetna, HCA Healthcare, Inc., and many others.[19]

48. PII and PHI have considerable value and constitute an enticing and well-known target to hackers. Hackers easily can sell stolen data as well as the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[20] PHI, in addition to being of

[19] HHS, *Cases Currently Under Investigation*, O.C.R. PORTAL, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited August 19, 2024).
[20] Brian Krebs, *The Value of a Hacked Company*, KREBS ON SECURITY (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

49. With respect to healthcare data breaches, another study found that "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft." The same study stated that "[a]ctors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures." [21]

50. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the United States. In 2023, there were 3,205 publicly disclosed data compromises, affecting over 353 million victims. The U.S. specifically saw a 72% increase in data breaches from the previous all-time high in 2021 and a 78% increase over the previous year.[22]

---

[21] Jessica David, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, HEALTH IT SEC. (Sept. 25, 2019), https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud.

[22] *2023 Data Breach Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2024), https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf.

51. Nuance, specifically, has a heightened awareness of its vulnerability to cyberattacks and the consequent risk of data breaches. In May 2023, Nuance experienced a security incident during which the PII and PHI of approximately 1.2 million patients, from thirteen different healthcare clients, were accessed and exfiltrated.[23]

52. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2019, roughly 3.5 million people reported some form of identity theft, fraud, or other consumer complaint compared to 5.4 million people in 2023.[24]

53. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[25]

54. "Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[26]

---

[23] Steve Alder, *Security Breaches in Healthcare in 2023*, HIPAA JOURNAL (Jan. 31, 2024), https://www.hipaajournal.com/security-breaches-in-healthcare/.
[24] *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFORMATION INSTITUTE, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Key%20Facts (last visited Aug. 15, 2024).
[25] *The Healthcare Industry is at Risk*, SWIVELSECURE https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited August 19, 2024).
[26] *Id.*

55. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and Class Members especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

56. As indicated by Jim Trainor, former second in command at the Federal Bureau of Investigation's ("FBI") cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[27] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[28]

57. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into

[27] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[28] *Managing Cyber Risks in an Interconnected World, Key Findings from the Global State of Information Security® Survey 2015*, PRICEWATERHOUSECOOPERS, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited August 19, 2024).

> your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.

58. Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[29]

59. According to the U.S. Government Accountability Office, which regularly reports its findings on information security: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to

[29] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

measure the harm resulting from data breaches cannot necessarily rule out all future harm."[30]

60. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

61. Based on the value of Plaintiff's and Class Members' PII and PHI to cybercriminals, Defendants certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

D. Defendants Breached Their Duty to Protect the PII and PHI with Which They Were Entrusted.

62. On or around November 29, 2023, GH detected unusual access to its patient information on its network server (the "Data Breach").[31]

[30] U.S. GOV'T ACCOUNTABILITY OFF., GAO-08-751, PERSONAL INFORMATION (2007).
[31] Notice, *supra* note 6.

63. GH determined that Nuance had failed to revoke a former employee's network access upon his termination. Using this access, the former Nuance employee accessed GH's patients' information on or around November 29, 2023—two days after the employee ceased working for Nuance.[32]

64. According to GH, it immediately notified Nuance of the Data Breach. Upon receiving this information from GH, Nuance finally disconnected the former employee's access to GH's records. Nuance then launched an investigation into the Data Breach.[33]

65. The investigation revealed that the former Nuance employee had compromised and stolen the personal information of more than 1 million GH patients.[34] The information compromised in the Data Breach includes a wide variety of patient PII and PHI, including *inter alia*, patient names in combination with one or more of the following: dates of birth, address, admit and discharge or transfer codes, medical record numbers, race, gender, telephone numbers, and healthcare facility names.[35]

66. Nearly seven months after the former Nuance employee initially gained access to patient information, GH began notifying individuals impacted by the Data

[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.*

Breach on or about June 24, 2024.[36] Shortly thereafter, Plaintiff received notice indicating that his PII and PHI was compromised during the Data Breach.

67. Upon information and belief, like Plaintiff, the Class Members received similar notices informing them that their PII and/or PHI was exposed in the Data Breach.

68. On or around this time, GH reported the Data Breach to the Department of Health and Human Services Office for Civil Rights' ("HHS") indicating that the Data Breach compromised the PII and PHI of approximately 1,276,026 individuals.[37]

69. Upon information and belief, the Data Breach occurred as a direct result of Defendants' failure to implement and follow basic security procedures in order to protect patients' PII and PHI.

E. Defendants are Obligated Under HIPAA to Safeguard PHI.

70. As discussed above, Defendants are required by the HIPAA, 42 U.S.C. § 1302d, *et seq*. to safeguard patient PHI.

71. HIPAA sets minim federal standards for privacy and security of PHI. HIPAA requires "compl[iance] with the applicable standards, implementation

[36] *Id.*
[37] HHS, *supra* note 19.

specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

72. Under 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

73. Under 45 C.F.R. § 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

74. HIPAA requires Defendants to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI they create, receive, maintain, or transmit; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by their workforces to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et. seq*.

75. HIPAA's security rules also require a covered entity to report a data breach without unreasonable delay and in no case later than sixty (60) calendar days from the discovery of the breach.[38]

76. HHS further recommends the following data security measures that regulated entities such as Defendants should implement to protect against some of the more common, and often successful, cyber-attack techniques:

a. Regulated entities should implement security awareness and training for all workforce members and that the training programs should be ongoing, and evolving to be flexible to educate the workforce on new and current cybersecurity treats and how to respond;

b. Regulated entities should implement technologies that examine and verify that received emails do not originate from known malicious site, scan web links or attachments included in emails for potential threats, and impeded or deny the introduction of malware that may attempt to access PHI;

c. Regulated entities should mitigate known data security vulnerabilities by patching or upgrading vulnerable technology infrastructure, by upgrading or replacing obsolete and/or unsupported applications and devices, or by implementing safeguards to mitigate known vulnerabilities until an upgrade or replacement can occur;

d. Regulated entities should implement security management processes to prevent, detect, contain, and correct security violations, including conducting risk assessments to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI; and

[38] *What are the HIPAA Breach Notification Requirements?*, HIPAA JOURNAL (Feb. 1, 2024), https://www.hipaajournal.com/hipaa-breach-notification-requirements.

e. Regulated entities should implement strong cyber security practices by requiring strong passwords rules and multifactor identification.[39]

77. Upon information and belief, Defendants failed to implement one or more of the above recommended data security measures.

78. While HIPAA permits healthcare providers and their business associates to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers or their business associates to disclose PHI to unauthorized third parties, nor did Plaintiff or the Class Members consent to the disclosure of their PHI to an unauthorized third party.

79. As such, Defendants are required under HIPAA to maintain the strictest confidentiality of Plaintiff's and Class Members' PHI that they require, receive, and collect, and Defendants are further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

80. Given the application of HIPAA to Defendants, and that Plaintiff and Class Members directly and/or indirectly entrusted their PHI to Defendants in order to receive necessary medical care, Plaintiff and Class Members reasonably expected that Defendants would safeguard their highly sensitive information and keep their PHI confidential.

---

[39] *OCR Quarter 1 2022 Cybersecurity Newsletter*, HHS (last updated Mar. 17, 2022), https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-first-quarter-2022/index.html.

F. Defendants Failed to Follow FTC Guidelines and Industry Best Practices.

81. Defendants are prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

82. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[40]

83. In 2016, the FTC updated its publication titled "Protecting Personal Information: A Guide for Business," which established cyber-security guidelines for businesses.[41] The guidelines recommend that business implement the following:

a. Businesses should promptly dispose of personal identifiable information that is no longer needed, and retain sensitive data "only as long as you have a business reason to have it;"

[40] *Start with Security: A Guide for Business*, FTC (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[41] *See Protecting Personal Information: A Guide for Business*, FTC, October 2016, available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited August 19, 2024).

b. Businesses should encrypt sensitive personal information stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;

c. Businesses should thoroughly understand the types of vulnerabilities on their network and how to address those vulnerabilities;

d. Businesses should install intrusion detection systems to promptly expose security breaches when they occur; and

e. Businesses should install monitoring mechanisms to watch for large troves of data being transmitted from their systems.

84. In another publication, the FTC recommended that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[42]

85. In another publication, the FTC recommended that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and

[42] *Start with Security: A Guide for Business*, *supra* note 40.

verify that third-party service providers have implemented reasonable security measures.[43]

86. Notably, the FTC treats the failure to employ reasonable data security safeguards as an unfair act or practice prohibited by Section 5 of the FTC Act. Indeed, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

87. Upon information and belief, Defendants failed to properly implement one or more of the basic data security practices recommended by the FTC. Defendants' failure to employ reasonable and appropriate data security measures to protect against unauthorized access individuals' PII and/or PHI constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

88. Similarly, the U.S. Government's National Institute of Standards and Technology ("NIST") provides a comprehensive cybersecurity framework that

[43] *Id.*

companies of any size can use to evaluate and improve their information security controls.[44]

89. NIST publications include substantive recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management strategies, access controls, training, data security controls, network monitoring, breach detection, and incident response.[45] Upon information and belief, Defendants failed to adhere to the NIST guidance.

90. Further, cybersecurity experts have identified various best practices that should be implemented by entities in the healthcare sector, including implementing the following measures to defend against common cyberattacks:

a. Email protection systems and controls;

b. Endpoint protection systems;

c. Identify all users and audit their access to data, application, systems, and endpoints;

d. Data protection and loss prevention measures;

e. IT asset management;

f. Network management;

g. Vulnerability management;

---

[44] *See Framework for Improving Critical Infrastructure Cybersecurity*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (April 16, 2018), App'x A, Table 2, available at https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf.
[45] *Id.* at Table 2 pg. 26-43.

h. Security operations center & incident response; and

i. Cybersecurity oversight and governance policies, procedures, and processes.[46]

91. Upon information and belief, Defendants' failure to protect massive amounts of PII and PHI is a result of their failure to adopt reasonable safeguards as required by the FTC guidelines, NIST guidance, and industry best practices.

92. Defendants were at all times fully aware of its obligations to protect the PII and PHI of patients because of their positions as a healthcare provider and a business associate, which gave them direct access to reams of patient PII and PHI. Defendants were also aware of the significant repercussions that would result from its failure to do so. Despite understanding the risks and consequences of maintaining inadequate data security, Defendants nevertheless failed to comply with their data security obligations, leading to the compromise of Plaintiff's and Class Members' PII and PHI.

G. Plaintiff and Class Members Suffered Damages.

93. For the reasons mentioned above, Defendants' conduct, which allowed the Data Breach to occur, caused Plaintiff and members of the Class significant injuries and harm in several ways. Plaintiff and members of the Class must immediately devote time, energy, and money to: (1) closely monitor their medical

[46] *HICP's 10 Mitigating Practices*, HHS, https://405d.hhs.gov/best-practices (last visited August 19, 2024).

statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

94. Once PII and PHI are exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendants' conduct. Further, the value of Plaintiff's and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

95. As a result of Defendants' failures, Plaintiff and Class Members are also at substantial increased risk of suffering identity theft and fraud or misuse of their PHI.

96. With respect to healthcare breaches, a study has found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[47]

[47] Jessica David, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, HEALTH IT SEC. (Sept. 25, 2019), https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud.

97. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[48]

98. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[49]

99. Health information in particular is likely to be used in detrimental ways – by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[50]

100. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[51]

101. Plaintiff and Class Members are also at a continued risk because their information remains in Defendants' systems, which have already been shown to be

---

[48] *Id*.
[49] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.
[50] *Id*.
[51] *The Potential Damages and Consequences of Medical Identity theft and Healthcare Data Breaches*, EXPERIAN (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

susceptible to compromise and attack and is subject to further attack so long as Defendants fail to undertake the necessary and appropriate security and training measures to protect the PII and PHI with which they were entrusted.

102. Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

H. Plaintiff's Experience.

103. Plaintiff Eric O'Brien is a patient of GH. Plaintiff was required to entrust his PII and PHI to GH in order to receive healthcare services. Upon information and belief, GH in turn entrusted his PII and PHI to Nuance.

104. In requesting and maintaining Plaintiff's PII and PHI, Defendants undertook a duty to act reasonably in their handling of Plaintiff's PII and PHI. Defendants, however, did not take reasonable care of Plaintiff's PII and PHI, leading to its exposure and compromise as a direct and proximate result of Defendants' inadequate data security measures.

105. On July 1, 2024, Plaintiff received notice that the PII and PHI that he directly and/or indirectly provided to Defendants was accessed and compromised in the Data Breach.

106. Since the occurrence of the Data Breach, Plaintiff has been required to spend his valuable time and effort in an attempt to mitigate any misuse of his PII and

PHI. These mitigation efforts include significant time and effort spent: (a) resetting the passwords to all of his accounts; (b) assessing the security of his bank and financial accounts; and (c) researching the Data Breach. Plaintiff would not have had to engage in these time intensive efforts but for the Data Breach.

107. Since the occurrence of the Data Breach, Plaintiff has been flooded with spam calls, which he did not have a problem with prior to the Data Breach.

108. Plaintiff has suffered actual injury from having his PII and PHI exposed and/or stolen as a result of the Data Breach, including: (a) mitigation efforts to prevent the misuse of his PII and PHI; (b) damages to and diminution of the value of his PII and PHI, a form of intangible property that loses value when it falls into the hands of criminals who are using that information for fraud or publishing the information for sale on the dark web; and (c) loss of privacy.

109. In addition, knowing that hackers accessed and likely exfiltrated his PII and PHI and that this information likely has been and will be used in the future for identity theft, fraud, and other nefarious purposes has caused Plaintiff to experience significant frustration, anxiety, worry, stress, and fear.

110. As a direct and proximate result of the Data Breach, Plaintiff has been and will continue to be at a heightened risk for fraud and identity theft and its attendant damages for years to come. Such a risk is real and certainly impending,

and is not speculative given the highly sensitive nature of the PII and PHI compromised in the Data Breach.

CLASS ALLEGATIONS

111. Plaintiff brings this Class Action on behalf of himself and all other similarly situated individuals pursuant to Rule 23 of the Federal Rules of Civil Procedure.

112. Plaintiff seeks to represent a class of persons to be defined as follows:

> All individuals in the United States whose PII and/or PHI was compromised in the Data Breach which was announced on or around June 24, 2024 (the "Class").

113. Excluded from the class are Defendants, their subsidiaries and affiliates, officers and directors, any entity in which Defendants have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

114. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when he moves for class certification, as necessary, to account for any newly learned or changed facts as the situation develops and discovery gets underway.

115. **Numerosity:** The members of the Class are so numerous that the joinder of all members is impractical. Plaintiff is informed and believes, and thereon alleges, that there are at least thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendants' records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes approximately one million individuals.

116. **Commonality:** This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether Defendants had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendants were negligent in collecting and storing Plaintiff's and Class Members' PII and PHI, and breached their duties thereby;

c. Whether Plaintiff and Class Members are entitled to damages as a result of Defendants' wrongful conduct; and

d. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct.

117. **Typicality:** Plaintiff's claims are typical of the claims of Class Members. Plaintiff's and Class Members' claims are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and Class Members each had their PII and PHI exposed and/or accessed by an unauthorized third party.

118. **Adequacy:** Plaintiff is an adequate representative of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the Class Members and has no interests antagonistic to the Class Members. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

119. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all Class members is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

120. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendants' liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendants breached their

duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

121. **Injunctive Relief:** Defendants have acted and/or refused to act on grounds that generally apply to the Class making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. R. Civ. P. 23(b)(2).

122. **Ascertainability:** Class Members are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through Defendants' books and records.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)
(Against Both Defendants)

123. Plaintiff restates and realleges the allegations set forth in every above paragraph as if fully set forth herein.

124. Defendants owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

125. Specifically, this duty included, among other things: (a) designing, maintaining, and testing Defendants' security systems to ensure that Plaintiff's and Class Members' PII and PHI in Defendants' possession was adequately secured and protected; (b) implementing processes that would detect a breach of their security

systems in a timely manner; (c) timely acting upon warnings and alerts, including those generated by their own security systems, regarding intrusions to their networks; and (d) maintaining data security measures consistent with industry standards.

126. Defendants' duty to use reasonable care arose from several sources, including but not limited to those described below.

127. Defendants owed a common law duty to Plaintiff and Class Members to implement reasonable data security measures because it was foreseeable that an unauthorized actor would target Defendants' data systems, software, and servers containing Plaintiff's and the Class's sensitive data and that, should a breach occur, Plaintiff and Class Members would be harmed. Defendants alone controlled their technology, infrastructure, and cybersecurity. They further knew or should have known that if an unauthorized actor breached their data systems, they would extract sensitive data and inflict injury upon Plaintiff and Class Members. Furthermore, Defendants knew or should have known that if hackers accessed the sensitive data, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and stolen. Therefore, the Data Breach, and the harm it caused Plaintiff and Class Members, was the foreseeable consequence of Defendants' unsecure, unreasonable data security measures.

128. Defendants also owed a common law duty because their conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendants' conduct included their failure to adequately restrict access to computer networks that held Plaintiff's and Class Members' PII and PHI.

129. Defendants' duty also arose from Defendants' positions as a healthcare provider and business associate. GH holds itself out as a trusted provider of healthcare, and thereby assumes a duty to reasonably protect its patients' sensitive information. GH directly provides comprehensive healthcare services and was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

130. Similarly, Nuance holds itself out as a trusted business associate of healthcare providers, and thereby assumes a duty to reasonably protect patients' PII and PHI. Nuance provides technology services to healthcare providers, including GH, and was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

131. Defendants breached the duties owed to Plaintiff and Class Members and thus were negligent. Defendants breached these duties by, among other things: (a) mismanaging their systems and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI;

(b) mishandling their data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards, key controls, systems, and procedures; (e) failing to evaluate and adjust their information security program in light of the circumstances alleged herein; and (f) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII and PHI.

132. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered injuries including:

a. Theft of their PII and PHI;

b. Costs associated with requesting credit freezes;

c. Costs associated with the detection and prevention of identity theft;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach;

g. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII and PHI being placed in the hands of criminals;

h. Damages to and diminution in value of their PII and PHI entrusted to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others; and

i. Continued risk of exposure to hackers and thieves of their PII an PHI, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff and Class Members.

133. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)
(Against Both Defendants)

134. Plaintiff restates and realleges the allegations set forth in every above paragraph as if fully set forth herein.

135. Pursuant to Section 5 of the FTC Act, Defendants had a duty to provide fair and adequate computer systems and data security to safeguard the PII and/or PHI of Plaintiff and Class Members.

136. Defendants breached their duties to Plaintiff and Class Members under Section 5 of FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII and/or PHI. Specifically, Defendants breached their duties by failing to employ

industry-standard cybersecurity measures in order to comply with Section 5 of the FTC Act, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

137. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendants or failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Defendants' duty.

138. It was reasonably foreseeable, particularly given the growing number of data breaches of PII and/or PHI within the healthcare industry, that the failure to reasonably protect and secure Plaintiff's and Class Members' PII and/or PHI in compliance with applicable laws would result in an unauthorized third-party gaining access to Defendants' networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted PII and/or PHI.

139. Plaintiff and Class Members are within the class of persons that Section 5 of the FTC Act is intended to protect.

140. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ

reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

141. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se.*

142. Furthermore, Defendants are Covered Entities under HIPAA, which sets minimum federal standards for privacy and security of PHI. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et. seq.*, and its implementing regulations, Defendants had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiff's and the Class members' electronic PHI.

143. Defendants violated HIPAA by actively disclosing Plaintiff's and the Class Members' electronic PHI; and by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI.

144. Plaintiff and the Class Members are patients within the class of persons HIPAA was intended to protect.

145. Moreover, the harm that has occurred is the type of harm that the HIPAA was intended to guard against.

146. Defendants' violation of HIPAA constitutes negligence *per se*.

147. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class Members have suffered injuries, including those identified in paragraph 132 above.

148. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)
(Against GH)

149. Plaintiff restates and realleges the allegations set forth in every above paragraph as if fully set forth herein.

150. Plaintiff and Class Members have an interest, both equitable and legal, in the PII and PHI pertaining to them that was conveyed to, collected by, communicated between, and maintained by GH and that was ultimately accessed or compromised in the Data Breach.

151. As a healthcare provider, GH has a fiduciary relationship with its patients, like Plaintiff and Class Members.

152. Because of that fiduciary relationship, GH was provided with and stored private and valuable PHI and PII related to Plaintiff and the Class. Plaintiff

and Class Members were entitled to expect their information would remain confidential while in GH's possession.

153. GH owed a fiduciary duty under common law to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in GH's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

154. As a result of the parties' fiduciary relationship, GH had an obligation to maintain the confidentiality of the information within Plaintiff's and the Class Members' medical records.

155. Patients, like Plaintiff and Class Members, have a privacy interest in personal medical matters, and GH had a fiduciary duty not to disclose medical data concerning the patients whose data they collect and maintain.

156. As a result of the parties' relationship, GH had possession and knowledge of confidential PII and PHI of Plaintiff and Class Members, information not generally known.

157. Plaintiff and Class Members did not consent to nor authorize GHS to release or disclose their PII and PHI to an unauthorized criminal actor.

158. GH breached its fiduciary duties owed to Plaintiff and Class Members by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and

integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to follow its own privacy policies and practices published to its patients; and (g) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

159. But for GH's wrongful breach of its fiduciary duties owed to Plaintiff and Class Members, their PII and PHI would not have been compromised.

160. As a direct and proximate result of GH's breach of fiduciary duties, Plaintiff and Class Members have suffered injuries, including those identified in paragraph 132 above.

161. As a direct and proximate result of GH's breach of its fiduciary duties, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Class)
(Against GH)

162. Plaintiff restates and realleges the allegations set forth in every above paragraph as if fully set forth herein.

163. Plaintiff and Class Members have an interest, both equitable and legal, in the PII and PHI pertaining to them that was conveyed to, collected by, communicated between, and maintained by GH and that was ultimately accessed or compromised in the Data Breach.

164. As a healthcare provider, GH has a special relationship with its patients, like Plaintiff and Class Members.

165. Because of that special relationship, GH was provided with and stored private and valuable PHI related to Plaintiff and the Class, which GH was required to maintain in confidence.

166. Plaintiff and the Class provided GH with their personal and confidential PHI under the express and/or implied understanding that GH would limit the use and disclosure of such PHI.

167. GH owed a duty to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PHI in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

168. GH had an obligation to maintain the confidentiality of Plaintiff's and Class Members' PHI.

169. Plaintiff and Class Members have a privacy interest in their personal medical matters, and GH had a duty not to disclose confidential medical information and records with which it was entrusted.

170. As a result of the parties' relationship, GH had possession and knowledge of confidential PHI and confidential medical records of Plaintiff and Class Members.

171. Plaintiff's and the Class's PHI is not generally known to the public and is confidential by nature.

172. Plaintiff and Class Members did not consent to nor authorize GH to release or disclose their PHI to an unauthorized actor.

173. GH breached the duties of confidence it owed to Plaintiff and Class Members when Plaintiff's and the Class's PHI was disclosed to the unauthorized actor.

174. GH breached its duty of confidence by failing to safeguard Plaintiff's and Class Members' PHI, including by, among other things: (a) mismanaging its systems and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of patient information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data

security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to follow its on privacy policies and practices published to its patients; (g) storing PHI and medical records/information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (h) making an unauthorized and unjustified disclosure and release of Plaintiff's and the Class Members' PHI and medical records/information to a criminal third party.

175. But for GH's wrongful breach of its duty of confidence owed to Plaintiff and Class Members, their privacy, confidences, and PHI would not have been compromised.

176. As a direct and proximate result of GH's breach of Plaintiff's and the Class's confidences, Plaintiff and Class Members have suffered injuries, including those identified in paragraph 132 above, and mental anguish accompanying the loss of confidences and disclosure of their confidential and private PHI, loss of their privacy and confidentiality in their PHI, and the erosion of the essential and confidential relationship between Defendants and Plaintiff and Class Members.

177. Additionally, GH received payments from Plaintiff and Class Members for services with the understanding that GH would uphold its responsibilities to maintain the confidences of Plaintiff's and Class Members' private medical information.

178. GH breached the confidence of Plaintiff and Class Members when it made an unauthorized release and disclosure of their confidential medical information and/or PHI and, accordingly, it would be inequitable for Defendants to retain the benefit at Plaintiff's and Class Members' expense.

179. As a direct and proximate result of GH's breach of its duty of confidences, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

FIFTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)
(Against Nuance)

180. Plaintiff restates and realleges the allegations set forth in every above paragraph as if fully set forth herein.

181. Plaintiff and Class Members have an interest, both equitable and legal, in the PII and PHI about them that was conveyed to, collected by, and maintained by Nuance and that was ultimately accessed or compromised in the Data Breach.

182. Plaintiff and Class Members conferred a monetary benefit upon Nuance in the form of monies paid for healthcare services or other services. Nuance's business model would not exist save for the need to ensure the security of Plaintiff's and Class Members' PII in order to provide technology services to its healthcare clients, such as GH.

183. The relationship between Nuance is not attenuated, as Plaintiff and Class Members had a reasonable expectation that the security of their PII and PHI would be maintained when they provided their PII and PHI to Nuance's customer, GH.

184. Nuance accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Upon information and belief, this financial benefit was, in part, conferred, when Nuance was paid by its clients, such as GH, to use Plaintiff's and Class Members' PII and PHI to provide technology services. Nuance also benefitted from the receipt of Plaintiff's and Class Members' PII and PHI.

185. Nuance also understood and appreciated that the PII and PHI pertaining to Plaintiff and Class Members was private and confidential and its value depended upon Nuance maintaining the privacy and confidentiality of the PII and PHI.

186. But for Nuance's willingness to commit to properly and safely collecting and maintaining the security of Plaintiff's and Class Members' PII and PHI, their sensitive information would not have been transferred to and entrusted to

Nuance. Further, if Nuance had disclosed that its data security measures were inadequate, Nuance would not have gained the trust of its healthcare clients, such as GH.

187. As a result of Nuance's wrongful conduct, Plaintiff and Class Members suffered damages in an amount equal to the difference between their payments made with reasonable data security and privacy practices and procedures that Plaintiff and Class Members paid for, and those payments without reasonable data security and privacy practices and procedures that they received.

188. Nuance's enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the collection, maintenance, and inadequate security of Plaintiff's and Class Members' PII and PHI, while at the same time failing to securely maintain that information from unauthorized access and compromise.

189. In particular, Nuance enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Nuance instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand,

suffered as a direct and proximate result of Nuance's decision to prioritize its own profits over the requisite security.

190. Nuance should not be permitted to retain the money belonging to Plaintiff and Class Members. It would be unjust, inequitable, and unconscionable to retain the benefits it received and is still receiving from Plaintiff and Class Members because Nuance failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal and state laws and industry standards.

191. The benefit conferred upon, received, and enjoyed by Nuance was not conferred gratuitously, and it would be inequitable and unjust for Nuance to retain the benefit.

192. Plaintiff and Class Members are without an adequate remedy at law.

193. Nuance should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Nuance should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Nuance's services, or Nuance should be compelled to place a percentage of all future profits into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, designed to represent the value obtained by the use of the inadequately secured PII and/or PHI compromised as a result of the Data Breach.

SIXTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)
(Against Both Defendants)

194. Plaintiff restates and realleges the allegations set forth in every above paragraph as if fully set forth herein.

195. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et. seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those here, that are tortious and violate the terms of the federal and state statutes described in this Class Action Complaint.

196. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII and PHI. Plaintiff alleges that Defendants' data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his PII and PHI and remains at imminent risk that further compromises of his PII and/or PHI will occur in the future.

197. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that, among other things:

a. Defendants owed a legal duty to secure patients' PII and PHI under the common law, Section 5 of the FTC Act, and HIPAA; and

b. Defendants breached and continue to breach this legal duty by failing to employ reasonable measures to secure patients' PII and PHI.

198. This Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect Plaintiff's and Class Members' PII and PHI.

199. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of any of Defendants' systems. The risk of another such breach is real, immediate, and substantial. If another breach of any of Defendants' systems occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

200. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants has a pre-existing legal obligation to employ such measures.

201. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach of Defendants' systems, thus eliminating the additional injuries that would result to Plaintiff, Class Members, and patients whose confidential information would be further compromised.

DEMAND FOR JURY TRIAL

Please take notice that Plaintiff demands a trial by jury as to all issues so triable in this action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, prays for relief as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

B. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

C. For compensatory damages on behalf of Plaintiff and the Class;

D. For punitive damages on behalf of Plaintiff and the Class;

E. For an order of restitution and all other forms of equitable monetary relief;

F. Declaratory and injunctive relief as described herein;

G. For disgorgement and/or restitution as the Court deems appropriate, just, and proper;

H. Awarding Plaintiff reasonable attorneys' fees, costs, and expenses;

I. Awarding pre- and post-judgment interest on any amounts awarded;

J. For reimbursement for all costs and expenses incurred in connection with the prosecution of these claims; and

K. Awarding of such other and further relief as may be just and proper.

Dated: August 19, 2024

Respectfully submitted,

/s/ Gary F. Lynch

Gary F. Lynch (PA 56887)
Jamisen A. Etzel (PA 311554)
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
gary@lcllp.com
jamisen@lcllp.com

Clifford A. Rieders, Esquire (PA 20962)
161 W. Third St.
Williamsport, PA 17701
(P) (570) 323-8711
(F) (570) 323-4192
Email: crieders@riederstravis.com

Attorneys for Plaintiff